SCOTT:
Secure COnnected Trustable Things

Demonstrator Generation 3

Document Type	Deliverable
Document Number	D12.6
Primary Author(s)	Andreas Springer | JKU
Document Version / Status	1.0 | Final
Distribution Level	PU (public)

Project Acronym	SCOTT
Project Title	Secure COnnected Trustable Things
Project Website	www.scottproject.eu
Project Coordinator	Michael Karner | VIF | michael.karner@v2c2.at
JU Grant Agreement Number	737422
Date of latest version of Annex I against which the assessment will be made	2020-03-09

SCOTT has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737422. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium, Norway.

CONTRIBUTORS

Name	Organization	Name	Organization
Andreas Springer	JKU	Rainer Hofmann,	TUG
Carlo Alberto Boano,	TUG	Kay Römer	TUG
Leander Hörmann	LCM	Peter Priller	AVL
Michal Tarkowski	GUT		

FORMAL REVIEWERS

Name	Organization	Date
Ramiro Robles	ISEP	2020-03-19
Michael Jerne	NXP AT	2020-03-27

DOCUMENT HISTORY

Revision	Date	Author / Organization	Description
0.1	2020-02-16	Andreas Springer / JKU	Template with task/activities assignment
0.2	2020-02-17	Carlo A. Boano / TUG	Added CTC demonstrator
0.3	2020-02-19	Leander Hörmann / LCM	Added OOB Demonstrator input
0.4	2020-03-03	Peter Priller / AVL	Added SOAK demonstrator
0.5	2020-03-12	Michal Tarkowski / GUT	Added 2 GUT demonstrators
0.6	2020-03-17	Leander Hörmann / LCM	Integrated LCM demonstrators
0.9	2020-03-17	Andreas Springer / JKU	Consolidation of inputs, finalized for review
1.0	2020-03-31	Andreas Springer / JKU	Addressed the reviewers comments

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 EXECUTIVE SUMMARY

This document describes the final status of the demonstrators of WP12. The implemented technologies are related to different aspects of wireless sensors communication (efficiency, security and interoperability) and localization. The structure of the document is as follows: in Chapter 2, objectives of the deliverable as well as reference to overall SCOTT objectives are given. Chapter 2.1 contains an analysis of the SCOTT requirements from the perspective of single demonstrators. All scenarios are listed and summarized in Chapter 3.1. Chapter 3.2 presents all demonstrators from WP12 using a predefined structure – first a detailed description of the respective demonstrator is given, then links to SCOTT Technology Building Blocks are presented in the Link to technology lines section and the Demonstrator public output section describes its availability to the public. In Chapter 4, related dissemination, exploitation and standardisation actions are summarized. Summary of references to SCOTT Technology Lines is given in Chapter 5. The document is concluded in Chapter 6 Conclusions.

Key words: demonstrator, wireless sensors communication, localization

2 OBJECTIVES

The main objectives of the document are as follows:

- Describe the SCOTT WP12 final demonstrators in detail
- Evaluate the fulfilment of the related SCOTT requirements
- Link the demonstrators with SCOTT Technology Lines and Technology Building Blocks

This deliverable, i.e. the described demonstrators support the realization of the **below listed SCOTT objectives**:

- **Focus on wireless systems**

WP12 demonstrators are based on wireless communication. The majority of developed demonstrators utilize wireless technologies as a major method of data transmission.

- **Focus on European leadership and market opportunities**

The results presented in this deliverable are based on real market needs, defined by WP12 Leader AVL. The demonstrators are based on cooperation between R&D and business entities, thus they have direct impact on European leadership and identification of market opportunities.

- **Focus on smart sensors and actuators**

In WP12, smart sensors and actuators are the main source of data. More details can be found in **Chapter 3.1**.

- **Focus on Security, Safety, Privacy and Trustability**

This objective is directly addressed in each demonstrator described in this document.

- **Focus on including psychological and socio-contextual enablers for trust formation**

This objective is addressed in the Trust Framework implementation in WP12, where socio-contextual issues are considered.

- **Focus on eco-system with well-defined re-usable Technical Building Blocks**

The description of the demonstrators and the whole environment is prepared from the perspective of SCOTT Technology Lines (TL) and Technology Building Blocks (TBB). A detailed mapping on TBBs is given in **Chapter 5** of this document.

- **Focus on solutions to be used in multiple industrial domains**

Interoperability of components developed under WP12 was taken into account from early stages of development. Moreover, several of the components are implemented in different work packages.

- **Focus on higher Technology Readiness Levels (TRLs)**

The TRL of components that build the WP12 environment is typically at levels 5-7.

2.1 Requirements fulfilment

This chapter describes how related requirements are fulfilled in each demonstrator. Currently some requirements are score only quantitatively. In those cases in which it is possible, a quantitative scoring of the achievements will be done during the final assessment.

2.1.1 Vehicle Conditioning (SOAK) Demonstrator – AVL

ID	BB	Short_name	Fulfilment
657	DemoRQ	Security Analysis	Initial analysis was done by JKU and SBA at the beginning of the project; update/refinement will be done with final demonstrator
658	DemoRQ	Robust WSN	Y2 prototype (Proto18A) has already proven its robustness when tested in soak room and other test bed environments; final Proto20 will be tested again --> OK
664	24.F	Deterministic and low latency	Already fulfilled with Y2 prototype (Proto18A) using EPHESOS protocol; it has proven time determinism and low latency in soak room and other test bed environments --> OK
673	24.F	Multi-scenario use	Test beds: proven, ok In-vehicle: shown in final soak room demonstrator
674	24.F	Multi-bubble scenario	Was not implemented due to shift in priorities
676	DemoRQ	Multi-sensor node	Pt100, Pt1000, TC: implemented and demonstrated. Pressure: will be shown in Proto20
677	DemoRQ	WSN node usability	A first version of Trustability indicator has been demonstrated in Y2/Proto18 already; will be extended for final Proto20
678	DemoRQ	System usability	Will be shown in Trustability indicator implemented in final Proto20

Table 1 Vehicle Conditioning demonstrator – fulfilment of requirements.

2.1.2 Demonstrator 3D Sensors positioning – GUT

ID	BB	Short_name	Fulfilment
390	23.P	Object localization and position	Localization system is able to operate at centimetre-level precision in various lighting conditions. Self-calibration algorithms are introduced to decrease the need of operators' assistance.
391	23.P	Localization_method	Distributed system allows for precise localization by various algorithms which works collaboratively to reduce possible errors, for example due to unexpected changes in cameras positions or changes in environment. Those problems, if not automatically solved, are redirected to notify a human operator.
552	23.P	Different_detecion_accuracy	Localization algorithm contains various pre- and post- processing algorithms, which increase accuracy, but extend overall localization time.
679	23.P	Location Based Security	The presence of the sensors is tracked by a specialized radio receiver which monitors RF spectrum for unexpected signals and abnormalities (like signal interferences).

Table 2 3D Sensors positioning – fulfilment of requirements.

2.1.3 Demonstrator CTC – TUG

ID	BB	Short_name	Fulfilment
627	24.F	Co-existing networks	Developed an enhanced cross-technology communication (CTC) scheme that allows to exchange unicast and broadcast messages between the most pervasive wireless technologies in the 2.4 GHz ISM band, namely IEEE 802.15.4 (ZigBee), Bluetooth Low Energy (BLE), and IEEE 802.11 (Wi-Fi). All these devices would normally be unable to interact due to their incompatible physical layer, and they are now empowered with the ability to directly communicate without the need of a dedicated gateway. Thanks to this novel CTC scheme, devices can coordinate the used frequency channels in order to reduce cross-technology interference and maximize coexistence.

ID	BB	Short_name	Fulfilment
628	24.F	Cross-technology-sync	Based on the aforementioned CTC scheme, a mechanism to synchronize the clocks of heterogeneous IEEE 802.15.4 and Bluetooth Low Energy devices at a microseconds-scale is currently being developed.

Table 3 CTC – fulfilment of requirements.

2.1.4 Demonstrator OOB Communication – LCM

ID	BB	Short_name	Fulfilment
431	23.F	Secure_key_exchange	Using Near Field Communication (NFC) as Out-of-band (OOB) communication channel, a key exchange is performed between an embedded computer and the sensor nodes.
522	23.F	Out_of_band_communication	Communication using a physical channel different to radio-communication. This is demonstrated using NFC using the nRF52832 IC and an embedded computer exchanging wireless network configuration data.
523	23.F	Localized_communcition	The OOB communication is only possible in a very reduced space. This is demonstrated as above using NFC.
525	23.F	Energy_efficiency_OOBCom	The OOB communication based on NFC is energy neutral regarding the wireless sensor node.
526	23.F	Robustness	The is demonstrated by evaluating the NFC in an industrial and automotive environment.
531	23.F	Latency_OoBCom	The latency requirements for the implemented OOB communication is demonstrated by applying the workflow of the use case (assigning and configuration of the sensor nodes for a measurement on the test bed) on the sensor nodes.

Table 4 OOB – fulfilment of requirements.

2.1.5 Demonstrator Energy Efficient Secure Communications – LCM/JKU

ID	BB	Short_name	Fulfilment
499	25.A	Secure_operation_cycle	The security concept is presented in the paper “Lifetime Security Concept for Industrial Wireless Sensor Networks” [8]. Furthermore, the communication protocol allows measures to ensure secure operation cycle but implementation for a full operation cycle is not possible within the time-frame of SCOTT.
500	25.A	Secure disruptions	Tamper detection implemented on hardware and integrated into trustworthiness indicator. Furthermore, the communication protocol allows measures to ensure secure disruption but implementation is not possible within the time-frame of SCOTT.
501	25.A	Out-of-band_security	See Table 4 OOB – fulfilment of requirements. The OOB system is used in this demonstrator.
502	25.A	Energy_efficiency	The new hardware for the sensor nodes (Proto20) will be demonstrated at the final event. Energy efficiency of hardware is ensured by using NFC as energy neutral communication regarding the wireless sensor node and by an energy-optimized software design.
504	25.A	Latency(2)	A determined latency is ensured by the communication protocol and it is demonstrated that the security concept has no degrading influence on it (see [8])

Table 5 Energy Efficient Secure Communications – fulfilment of requirements.

3 DESCRIPTION OF WORK

3.1 Demonstrators links to Use Case Scenarios

All demonstrators described in this deliverable refer to the use case “Ubiquitous Testing of Automotive Systems” which is described into detail in D12.1 Use Case Specification "Ubiquitous Testing of Automotive Systems" [10]. In D12.1 in total 8 specific scenarios within this use case were described. In Table 6 it is listed, which demonstrator addresses which use case scenario.

Scenario No.	Scenario Name	Demonstrator Name	Organization
1	Instrumentation and hot testing of an Unit under test (UUT)	Vehicle Conditioning (SOAK) demonstrator	AVL
2	Localization of Sensors and automatic deduction of context	Multimodal Positioning System (MPS)	GUT
3	Mount UUT into a test bed (or vehicle) and check setup	OOB Communication	LCM
4	Run tests (operate and monitor UUT, test bed/vehicle and measurement system)	Vehicle Conditioning (SOAK) demonstrator Energy Efficient Secure Communications	AVL LCM/JKU
5	Define, manage and evaluate test	Shown using the Vehicle Conditioning (SOAK) demonstrator (#1)	AVL
6	Configure, check and run a distributed test setup, combining two or more parts of a UUT	Cross-technology communication (CTC)	TUG
7	Check, maintain and calibrate measurement system	Shown using the Vehicle Conditioning (SOAK) demonstrator (#1)	AVL
8	Produce and maintain measurement system	Shown using the Vehicle Conditioning (SOAK) demonstrator (#1)	AVL

Table 6 Use Case Scenarios link to Demonstrators

3.2 Demonstrators description

3.2.1 Demonstrator Vehicle Conditioning (SOAK) demonstrator – AVL

During the run of project SCOTT, partners identified the specific use case suited best for demonstrating advantages of a wireless instrumentation system: a chassis dyno (CD) test bed and its soaking facilities for pre-conditioning. CD test beds are typically rooms large enough to accommodate complete vehicles plus all necessary equipment. They are used to verify full-vehicle behaviour, including NVH (noise, vibration, harshness), EMC, powertrain efficiency etc.

Since the EURO 6 regulation, vehicle testbeds are also used more and more often to verify vehicle's emissions behaviour, as regulators now require having real-vehicle, real-driving tests for realistic measurements. This includes well-defined conditioning of the vehicle (e.g. temperature). As a result, vehicles will be pre-conditioned in specific rooms (called soak-rooms – hence the name of the demonstrator). This needs to be monitored and documented, typically by cyclically measuring and storing temperature in certain points of the vehicle, like oil sump, coolant heat exchanger, etc. As vehicles need to move between soak rooms and test beds, wireless instrumentation is highly preferable. The final demonstrator of AVL will thus cover such a setup. A vehicle will be instrumented with a couple of sensor nodes (goal: 5) which will connect to a base station placed in the test bed. In this use case, the vehicle will move between the soak room and test bed, demonstrating range, coverage and robustness of the WSN.

As an additional feature, the "doorstep localization" will be demonstrated as well. For documentation of the test sequence, it is necessary to precisely identify and log the moment when the vehicle moves from the soak room (or area) to the test bed, thus "crossing the doorstep". This will be identified in the WSN by a newly developed functionality by JKU, which is based on identification of RSSI fluctuations in the network.

An important part will be the final realization of trustability indicators, allowing users to understand system state and behavior in order to allow acceptance of innovations like WSN-based measurement systems. The final demonstrator will thus use and extend the trustability indicator pre-viewed in the Y2 review. The goal of SCOTT is to prove robustness, dependability and thus trustability of wireless systems in challenging industrial environments. This demonstrator shall show maturing the technical building blocks with targeted TRL of 6-7. This demonstrator is expected to also support exploitation activities for all partners.

The demonstration will be shown at the acoustics testbed of AVL in Graz, Austria (see Figure 1). Main dimensions test bed: L x W x H = 14000 x 16000 x 5500 mm

Figure 1 AVL acoustics chassis dyno test bed (Graz, Austria)

3.2.1.1 Link to technology lines

There is are only minor changes / clarifications in the mapping / use of building blocks from SCOTT's technology lines compared to D12.4, in chapter "3.2.1.1 Link to technology lines"

The following Table 7 lists the TL/BB applied in this demonstrator:

BB	Name	Description	Organization in charge
23.C	Hardware supported Security Mechanism	Implemented (HW encryption in WSN nodes)	LCM, JKU
23.F	Out of Band Security	Integrated, for authentication of nodes, and to join/unjoin networks	LCM
23.G	PHY Layer Security	Integrated, will be used as a component to the trust indicator	JKU
23.N	SCOTT security lib	Concept for using mbedTLS	AVL, NXP
23.P	Spatial-based authorization and authentication	Concept exists	GUT, AVL

BB	Name	Description	Organization in charge
23.F	Trust Anchor for ES smart sensors	Concept exists	JKU, LCM, AVL, NXP
24.B	Addressing and mobility management of sensors/actuators	shown in “doorstep localization” in this demonstrator	JKU
24.F	Cross-technology synchronization	Will be presented in own demonstrator	TUG
25.A	Energy efficient security implementation in WSN's	Provides energy-efficient encryption shown in this demonstrator	JKU
25.B	Energy efficient & resource optimized component concepts for WSNs	shown in Proto20	JKU, LCM, NXP
25.C	Energy storage for WSNs	Concept exists	LCM
25.F	In-vehicle WSN	Shown in soak-room test setup	LCM

Table 7 TL/Building Blocks applied in the Vehicle soak demonstrator

3.2.1.1 Demonstrator public output

Due to safety regulation, automotive test beds are typically in restricted areas. This is also the case for the demonstrator in the chassis dyno test bed at AVL. It will be accessible for the final review by consortium partners, reviewers and JU officers only.

In order to provide material for public dissemination however, AVL will produce a movie and pictures and make it available via SCOTT’s dissemination channels (website, social network, ...)

3.2.2 Demonstrator 3D Sensors positioning – GUT

This demonstrator presents precise localization of sensors in 3D space using a specialized, distributed cameras system. By using self-contained smart devices, one can determine the position and unique identifier of visual tags placed on the engine. Each device consist of a microcomputer with Raspberry Pi and a camera with a lens. Additionally it uses two wireless connections: WLAN (WiFi) for data transfer (mostly diagnostics and results) and a WSN node for triggering synchronized localization procedure. Camera can be powered by embedded battery or 5V micro USB port.

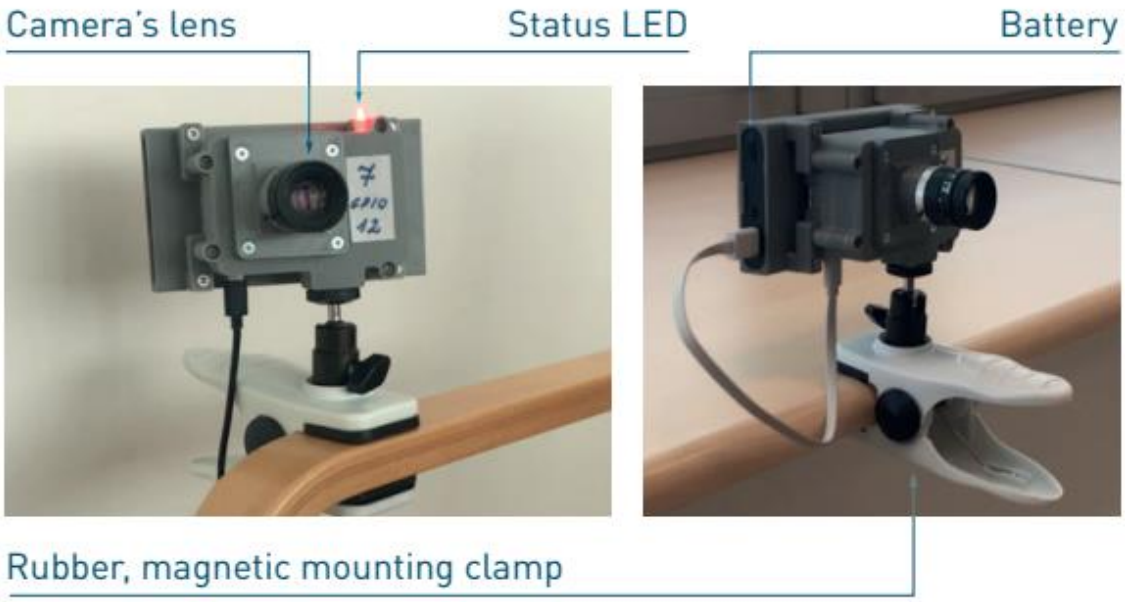

Figure 2 Camera device used in 3D localization demonstrator

Specialized tags are tied to the physical sensor which position is meant to be localized. Both cameras and sensors are connected by a wireless, synchronized network based on the EpHESOS protocol to maintain time dependencies during triggering of the localization procedure. Each camera acts as edge computing device running all possible computer vision algorithms to provide high expandability of the system. In this approach the accuracy and coverage of the system can be improved by adding more cameras without increasing demand on time or external hardware resources. Sensor localization can be treated as a service with rich API available to access all its functions and receiving results. In this demonstrator a web application is used to show the whole procedure along with intermediate results.

Figure 3 Localization sensor used in 3D localization demonstrator

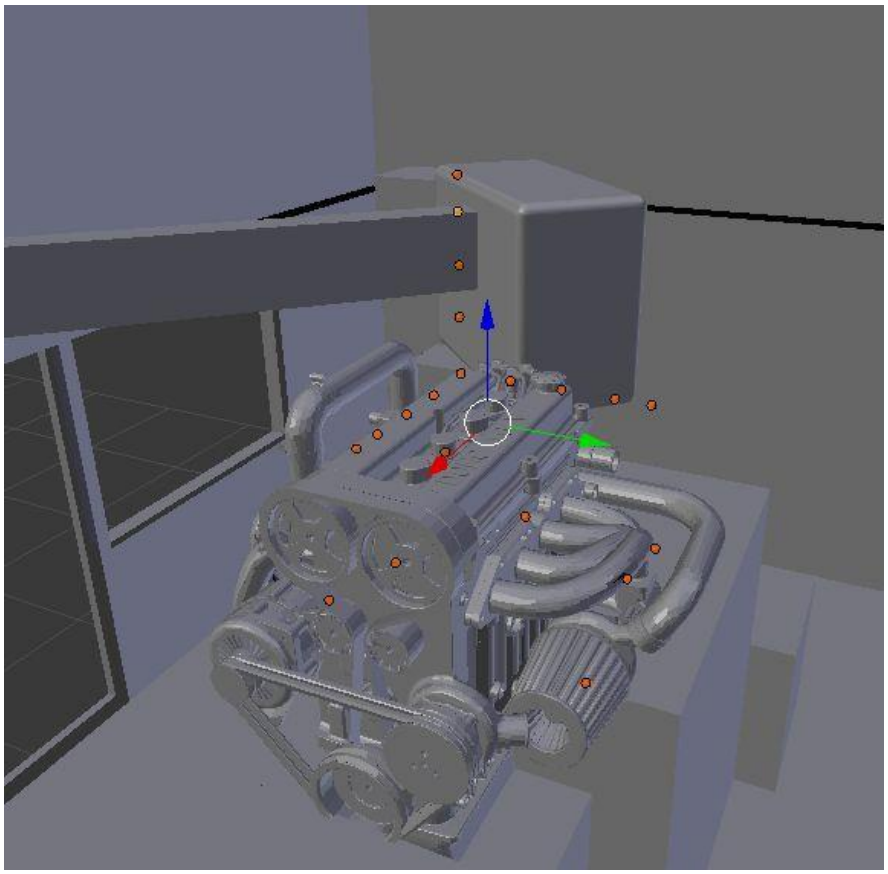

Figure 4 Visualization of localization results

3.2.2.1 Link to technology lines

BB23.G	PHY Layer Security
BB23.P	Spatial-based authorization and authentication

The 3D sensor localization demonstrator, addresses Building Block 23.P „Spatial-based authorization and authentication“ by using localization techniques to identify sensors in 3D space. It is also connected with Building Block 23.G „PHY Layer Security“, as localization information can be regarded as a physical layer feature, which can be used for security measures.

3.2.2.2 Demonstrator public output

3D sensor localization demonstrator will be presented in public in reduced form, with less camera devices and smaller scale.

3.2.3 Jamming detection and counteraction demonstrator – GUT

The second demonstrator developed by GUT focuses more on the communication security – the concept of jamming detection in WSN (Wireless Sensor Network). It consists of two sensors using the 802.15.4 standard (transmitter and receiver), a jamming device and a so-called extended receiver (eRX). During the communication, the jamming device is turned on. The extended receiver is able to detect the interference which allows for a reaction of the system. One of the sensors is

equipped with a specialized, reconfigurable antenna which can change its radiation pattern to mitigate jamming source and maintain the communication.

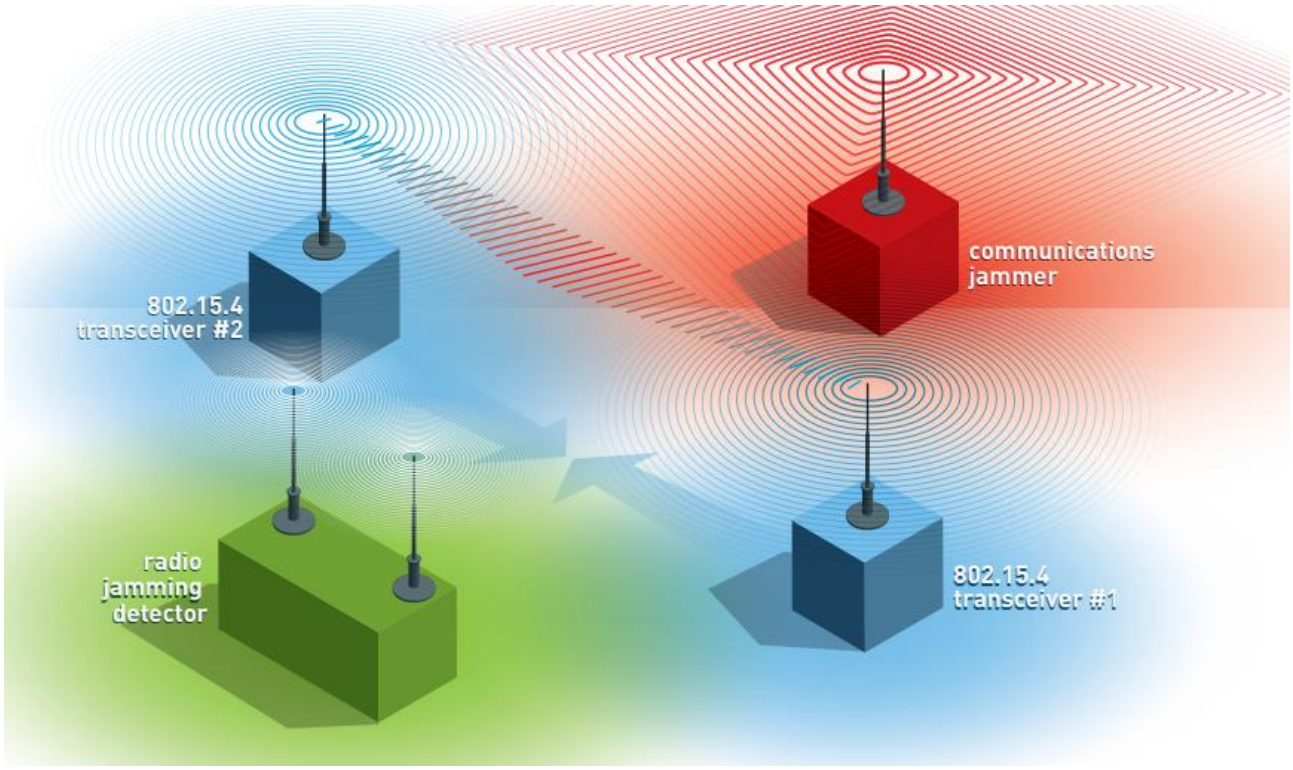

Figure 5 Visualization of the jamming detection and counteraction demonstrator

3.2.3.1 Link to technology lines

BB23.F	Out of Band Security
BB23.G	PHY Layer Security
BB23.P	Spatial-based authorization and authentication

3.2.3.2 Demonstrator public output

The jamming mitigation will be presented with a reduced form (with less signal power), so not every feature will be demonstrated, but overall concept will be shown. Additionally, movies with convenient explanations will be displayed on screen during the public event.

Concerning the scientific output, two conference papers were presented: “Investigation of Continuous Wave Jamming in an IEEE 802.15.4 Network” [6] on 2018 22nd International Microwave and Radar Conference (MIKON)/ IEEE and „Validation of a virtual test environment for C2X communication under radio jamming conditions“ [7] on 2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE).

3.2.4 Demonstrators Cross-Technology Communication – TUG

TUG implemented two demonstrators showcasing work on cross-technology communication (CTC).

Demonstrator 1. In a first demonstrator, we presented a generic CTC scheme allowing bidirectional communication between off-the-shelf IoT devices operating in the 2.4 GHz band. In particular, we make use of and extend the X-Burst framework [1] presented in the previous deliverables to enable a broadcast communication between devices embedding a Wi-Fi, BLE, or IEEE 802.15.4 radio. X-Burst encodes data in the duration of energy bursts by transmitting legitimate frames with different payload lengths [1]. Devices with incompatible physical layer, but operating on overlapping channels, can detect the energy bursts and decode information by sampling the received signal strength at a high frequency. As the transmission of frames with variable size and energy detection are features available in most off-the-shelf IoT devices, X-Burst is not technology-specific and allows to broadcast cross-technology frames to multiple devices using diverse technologies simultaneously without the need of expensive and inflexible gateways.

Compared to the demonstrator of Y2, we have added the Raspberry Pi 3B+ to the platforms supported by X-Burst, thus enabling off-the-shelf Wi-Fi, BLE, and IEEE 802.15.4 devices to broadcast CTC frames to each other simultaneously. In X-Burst, the implementation of CTC functionality (e.g., the encoding and decoding of symbols, as well as the assembly/disassembly of frames) is separated from platform-specific details using a hardware abstraction layer (HAL), as shown in Figure 6. This ensures a high portability of the framework: the HAL of each platform needs to expose how to (i) generate bursts of different length, (ii) sample the RSS, and (iii) fine-tune the radio's transmission power. We have previously integrated X-Burst into the Contiki OS, and supported several off-the-shelf IoT platforms embedding BLE or IEEE 802.15.4 radios, such as the TI CC2650 LaunchPad, Zolertia Firefly, and TelosB nodes [2].

To enable a CTC between these platforms and an off-the-shelf Wi-Fi device, we have now also implemented and ported X-Burst to the popular Raspberry Pi 3B+. Since the Raspberry Pi 3B+, as most Wi-Fi devices, does not expose support for frame injection and RSS sampling by default, a firmware modification is required. The BCM43455c0 radio used on the Raspberry Pi 3B+/4B series has recently been reverse-engineered, and it is now possible to replace code down to individual instructions within the firmware and exploit the unused memory to implement new functionality using the Nexmon patching framework. JamLab-NG is built on top of Nexmon and extends its frame injection functionality by disabling the CCA and by avoiding other sources of entropy such as the operating system's network stack. We use JamLab-NG's jelly tool to create energy bursts by injecting frames of custom length at a fixed transmission speed without the need to connect to an access point.

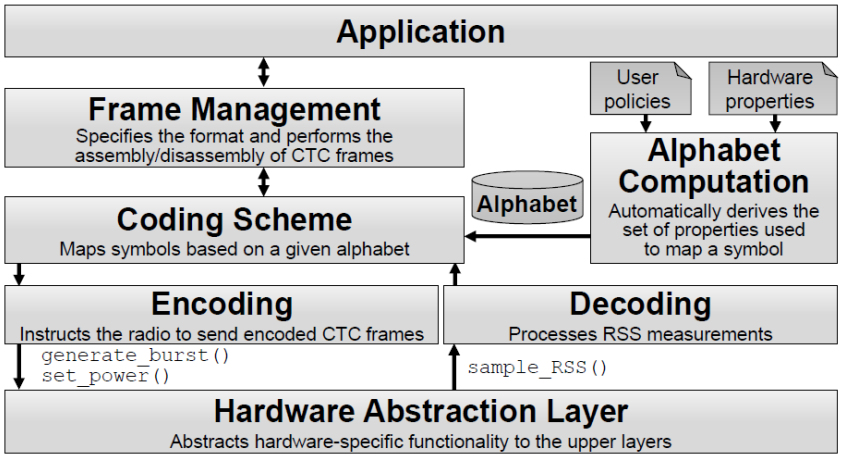

Figure 6 X-Burst's architecture (adapted from [1])

We have further extended JamLab-NG's low-level interface from the kernel to the firmware (ioctls) to trigger an existing energy detection function within the BCM43455c0 and return its result to a userland application through the kernel's network stack. To enable a cross-technology data exchange, we map data symbols into energy bursts of pre-defined duration. In our implementation, we make use of a 2-bit coding scheme and specify four burst durations, namely: 224, 416, 608, and 800 µs. These values are chosen based on the properties of the employed hardware platforms (such as the RSS sampling frequency and time granularity), such that every device performing CTC is able to correctly distinguish two different energy burst durations by means of RSS sampling [1].

The demonstrator setup is illustrated in Figure 7: we make use of four off-the-shelf IoT platforms supporting X-Burst, namely: TI CC2650 LaunchPad (BLE), Raspberry Pi 3B+ (Wi-Fi), Zolertia Firefly (IEEE 802.15.4), and TelosB mote (IEEE 802.15.4). Each device is equipped with four LEDs of different colours, where each colour is associated to a device (e.g., red→Firefly; green→TelosB). Each device is also equipped with three buttons, two of which allow to turn on/off the LED associated to that specific device by initiating the transmission of a broadcast CTC frame. The third button allows to initiate the transmission of several CTC broadcast frames back-to-back in order to compute the throughput to all nearby devices. All communications are monitored, logged, and displayed using a laptop connected via USB to each device, as well as a PicoScope, so to gain a more detailed insight about X-Burst's encoding process.

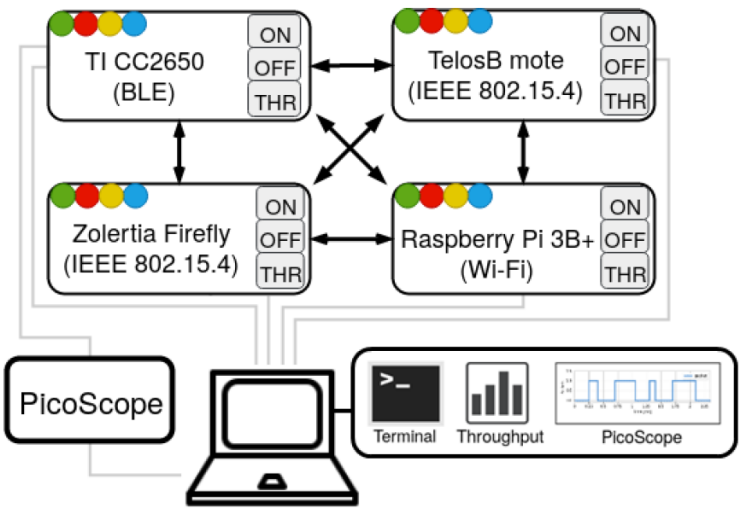

Figure 7 Demonstration setup: several BLE, Wi-Fi, and IEEE 802.15.4 devices broadcast CTC frames to control each other's LEDs. Real-time info about the throughput is displayed on a display / laptop

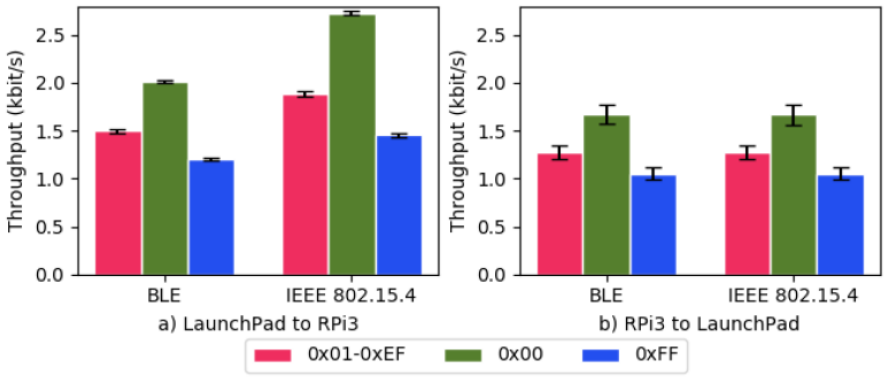

Figure 8 Data throughput between TI CC2650 LaunchPad & Raspberry Pi 3B+ for different payloads

We have also evaluated the throughput experimentally between a Raspberry Pi 3B+ and a TICC2650 LaunchPad in both BLE and IEEE 802.15.4 mode. Figure 8 shows our results: the TI CC2650 LaunchPad and the Raspberry Pi 3B+ can exchange CTC messages at up to 2.5 kbit/s, depending on the payload content (values such as '0x00' are encoded in shorter durations than '0xff' and hence transmitted faster) as well as the technology used. The relative differences in throughput between the various technologies are due to the different radio preparation time of each platform (i.e., the time elapsed between the transmission of two consecutive frames).

Demonstrator 2. In a second demonstrator, we showcase the clock synchronization of BLE and IEEE 802.15.4 devices. To this end, we have extended X-Burst and built X-Sync, a protocol that enables the transmission and reception of timestamps. X-Burst traditionally encodes information in the duration of legitimate packets by transmitting a CTC frame embedding a preamble (used by receivers to detect the presence of a CTC transmission) and a payload containing the actual data to be exchanged. X-Sync adds an additional preamble after the original X-Burst preamble to accurately determine the beginning of the CTC frame, as explained below, and transmits a device timestamp as part of the X-Burst payload. The accuracy of a synchronization scheme is primarily limited by the delays added during the transmission and reception process: Figure 9 shows these delays in detail.

Traditionally, the end-to-end latency when exchanging a timestamp equals l_1, i.e., it is computed from the instant in which the application issues the message embedding the timestamp to the instant in which the latter is decoded by the receiver. To get rid of non-deterministic delays introduced by the OS and network stack (send / receive time in Figure 9), as well as by the medium access control scheme (access time), X-Sync uses MAC timestamping, where timestamps are generated by reading the local clocks immediately when a message is sent or received. The sampling and processing speed of RSS values is limited by the used hardware and strongly varies among platforms. To compensate the sampling delay and thus, to minimize the variability of the end-to-end latency, each CTC frame contains a well-known sequence of legitimate packets (X-Sync preamble). This sequence is used to accurately determine the beginning of a CTC frame. To this end, X-Sync samples the RSS only at specific points in time and predicts the beginning of the next packet within the X-Sync preamble. Depending on the sampled value, i.e., if a packet was detected (RSS ≥ threshold) or not (RSS < threshold), the instant of time in which the next RSS value is sampled is adjusted accordingly. That is, if no packet was detected, the RSS sampling point was chosen too early and hence the next RSS sampling point will be slightly postponed (and vice-versa). This process, which is called repetitive sampling, is repeated until the last packet of the X-Sync preamble is reached. Since the nominal durations of all previously-received packets and gaps are known, the start of the CTC frame can be determined and the sampling delay compensated accordingly.

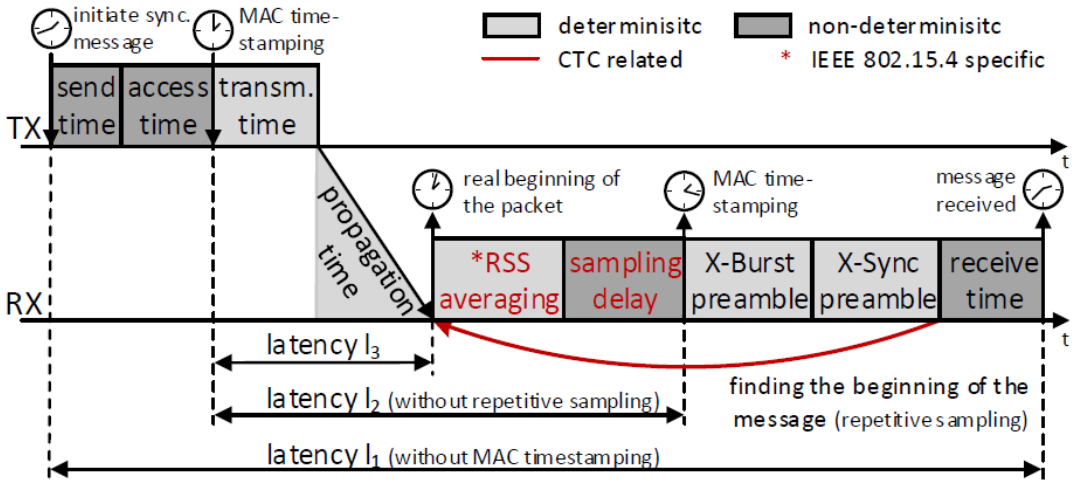

Figure 9 Our approach for cross-technology synchronization

IEEE 802.15.4 devices experience a constant, device-dependent offset caused by the averaging of the RSS values. In particular, depending on the used threshold and setup, the detection of packets is delayed up to 128 µs. Therefore, the calculated start of the CTC frame has to be corrected by a constant, measurable factor. To reduce the number of synchronization messages and thus the energy consumption, X-Sync estimates the clock drift between two devices using linear regression. This way, after sufficient data points are collected, the synchronization interval can be increased. To improve precision, we apply filtering on the received timestamps using random sample consensus (RANSAC).

We have implemented X-Sync using Contiki-NG on three off-the-shelf IoT devices: the TI CC2650 LaunchPad, the Zolertia Firefly, and the TelosB mote. To evaluate the accuracy of X-Sync, we use the CC2650 LaunchPad in BLE and IEEE 802.15.4 mode to transmit its clock to various IEEE 802.15.4 and BLE devices, respectively. We use a synchronization interval of 10 s and measure the error as the maximum deviation over a time of 1000 s at a rate of 1 Hz. Additionally, a constant

factor was used to compensate static delays (transm. / propagation time in Figure 9). Figure 10 shows our initial results. The high variance on the TelosB mote is due to its limited RSS sampling rate and processing power.

Platform		Sync. Error [μs]		
TX	RX	Min	Median	Max
CC2650 (BLE)	CC2650 (IEEE)	-0.64	-0.20	0.68
	Zolertia Firefly	-0.84	-0.13	0.25
	TelosB mote	-40.32	9.21	197.9
CC2650 (IEEE)	CC2650 (BLE)	-0.83	0.54	1.65

Figure 10 An evaluation on IEEE 802.15.4 and BLE devices shows that X-Sync can achieve sub-µs-level accuracy

3.2.4.1 Link to technology lines

The CTC component is related to BB24.F (cross-technology synchronization), as it allows wireless devices using heterogeneous technologies (e.g., IEEE 802.15.4, BLE, and Wi-Fi) to directly exchange data in both directions without gateways, and hence to synchronize their operations. Such CTC component can be used to coordinate the used frequency channels among heterogeneous wireless devices in order to maximize coexistence, as well as to synchronize the clocks of heterogeneous wireless devices at a microseconds-scale.

3.2.4.2 Demonstrators public output

A scientific publication describing X-Burst's enhanced architecture in detail, as well as the successful transmission of broadcast and unicast CTC messages between multiple heterogeneous IEEE 802.15.4 and BLE platforms (the CC2650 Launchpad, the Advanticsys MTM5000-MSP, and the Zolertia Firefly) was presented at the SECON'19 conference [1].
A public demonstration showing X-Burst's ability to broadcast cross-technology frames between off-the-shelf Wi-Fi, BLE, and IEEE 802.15.4 devices was presented at the EWSN'20 conference [2]. Furthermore, a poster presenting our initial results on cross-technology synchronization between BLE and IEEE 802.15.4 devices was presented at the EWSN'20 conference [3].

3.2.5 Demonstrator OOB Communication – LCM

The out-of-band (OOB) communication demonstrator shows the secure communication mechanisms based on OOB communication. The OOB communication enhances the overall security of a communication system by adding a special communication channel with certain properties. These properties typically include a short and well-known communication range and a different physical layer than the main communication channel. The additional channel is used to exchange secret information for example a cryptographic key or the sensor node configuration. This enables an encrypted communication over the public accessible network without the possibility of a man-in-the-middle attack. Figure 11 shows an overview of the OOB communication demonstrator.

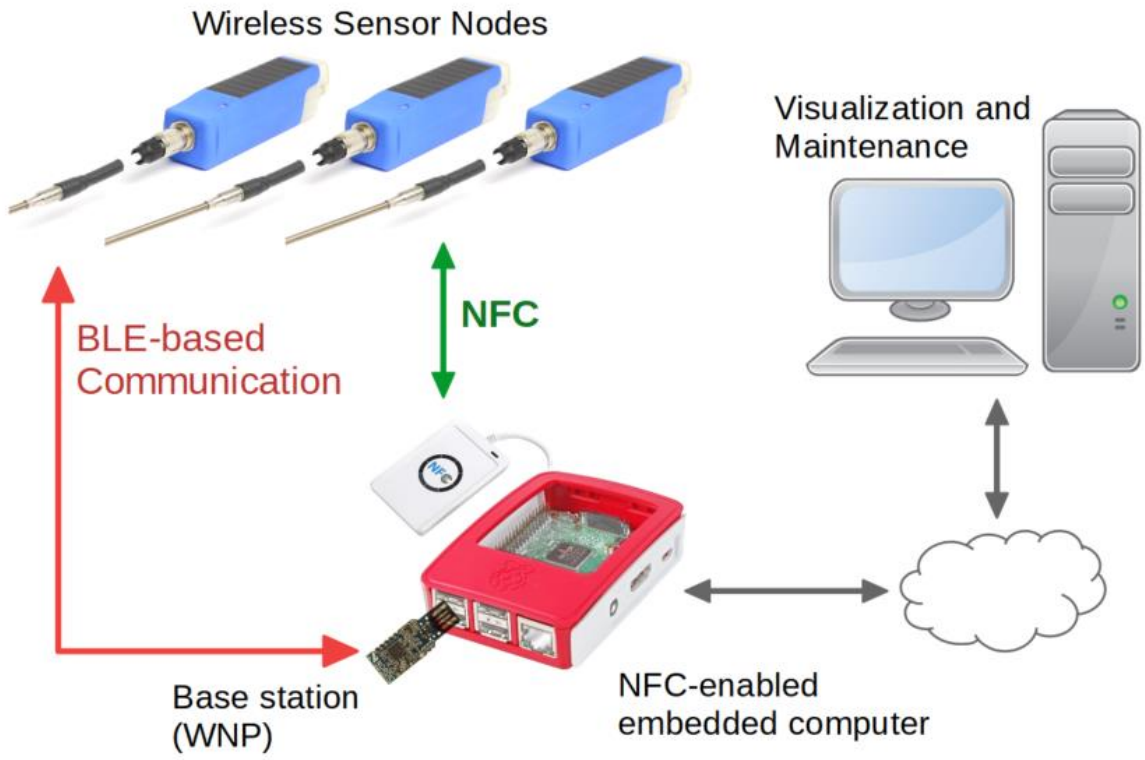

Figure 11 Principle structure of the OOB demonstrator

The OOB demonstrator shows the OOB communication using Near-Field-Communication (NFC) as an additional communication channel between the embedded computer (Raspberry PI 3B+) and the wireless sensor nodes. The wireless sensor nodes are used to measure temperature of Pt100, Pt1000 or Thermocouple sensors. The software was adapted in this project to fulfil the requirements of NFC-based OOB communication. The main purpose of the OOB communication is to perform a secure key exchange between the embedded computer and the sensor nodes. The key is handed over to the wireless network processor (WNP) which will communicate over the unsecure Bluetooth-Low-Energy (BLE) physical layer using the key. Thus, the communication is secured against data tampering, impersonation and information disclosure. This procedure will be visualized using textual and graphical output on a PC. Energy efficiency is very important to operate the wireless sensor nodes as long as possible. The energy efficiency is ensured by the use of NFC since this is an energy neutral communication regarding the wireless sensor nodes (acting as passive NFC tags).

3.2.5.1 Link to technology lines

The demonstrated OOB communication setup will be integrated into the use case demonstration “Automotive Instrumentation System – WSN”. It uses BB23.F (OOB communication) and parts from BB25.F (In-Vehicle WSN). It will be used to assign sensor nodes to a measurement setup (a specific wireless network) and to exchange secure information e.g. secret keys and sensor configuration.

3.2.5.2 Demonstrator public output

The OOB communication is part of the security concept developed in BB25.F. This security concept has been acceted for publication at the “16th IEEE International Conference on Factory Communication Systems”.[8]

3.2.6 Demonstrator Energy Efficient Secure Communications – LCM/JKU

Based on the WSN prototype for automotive verification and validation from the predecessor project DEWI, this demonstrator provides security mechanisms for efficient, dependable and energy autonomous WSN systems for local instrumentation of UUT's. This demonstrator is based on the EpHESOS communication protocol [4] and uses the Bluetooth Low Energy PHY. We added encryption using the AES128 ECB/CCM standard method, as offered by the transceiver chip used in the already existing automotive testbed application. Each transmitted data packet contains a Message Integrity Code (MIC) for authentication. Each MIC is 4-8 byte long and usually generated automatically by the transceiver hardware. Encryption is applied to secure the communication between the nodes and the base station. The nodes and the base station exchange parameters relevant for the communication such as channel timing, which need to be kept secret to increase the security level (represented by the grey arrows in Figure 12). End to end security is guaranteed to protect the measurement data sent to the PLC from being eavesdropped, altered or disturbed. The base station can be a transparent hop for the data or data have to be repacked in a newly secured communication line to the automation system (represented by the grey arrows in Figure 12).

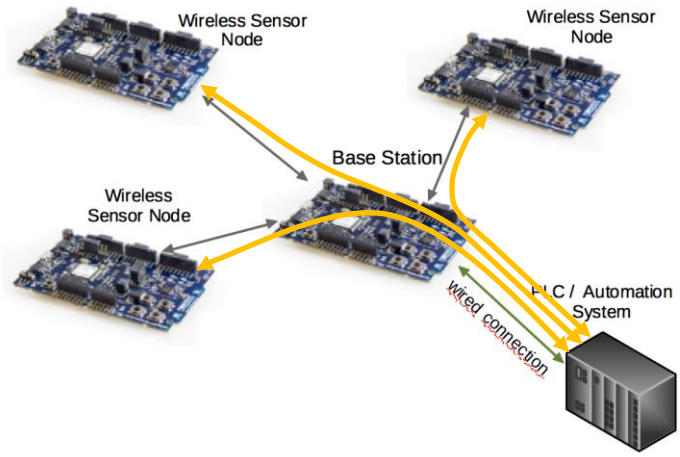

Figure 12 Secure communication links between nodes and base station and automation system

The exchange of keys for the AES128 ECB/CCM encryption standard is performed via out-of-band communication using NFC as described in section 2.1.4 "Demonstrator OOB Communication – LCM".

For combating jamming attacks, which are equivalent to denial-of-service attacks, we have developed the BASEBAL (**BA**ckward **S**tructured **E**nergy **BA**lanced **L**ink) combined routing and network concept with integrates security and considers an energy efficient implementation. Moreover, constraints such as defined low latency contribute to the complexity, but also point a way to the solution of the problem. The implementation of the BASEBAL routing algorithm consists of two parts: (1) Network discovery and (2) network link phase. The network is organized in layers. The nodes of layer *n* are connected to nodes of layer *n-1* and *n+1*. In layer 0 only the base station is considered. Nodes that can receive beacons transmitted from BS are considered to be in layer 1. Next, considering the layer 1 nodes as relay, the beacons transmitted from the base station can now be relayed further. Thus, all nodes who receive the beacons at this stage are considered as part of layer 2. The network discovery continues until all nodes are discovered and sorted into

layers. The implementation of the BASEBAL routing algorithm as described in [5], follows the network discovery step. All possible routes start at the base station and each route connects one node out of the total amount of nodes in the network. The algorithm starts at the last layer and navigates backwards.

The SNR of the wireless link is used as quality parameter and in parallel as indicator for ongoing attacks or vulnerability. The Packet Error Rate (PER), the inter-node synchronization and the end to end synchronization indicate whether a connection between two nodes or within a path is suspicious or not. If the location of the nodes is known, routing contributes to localize the position of the disturbance. (Figure 13).

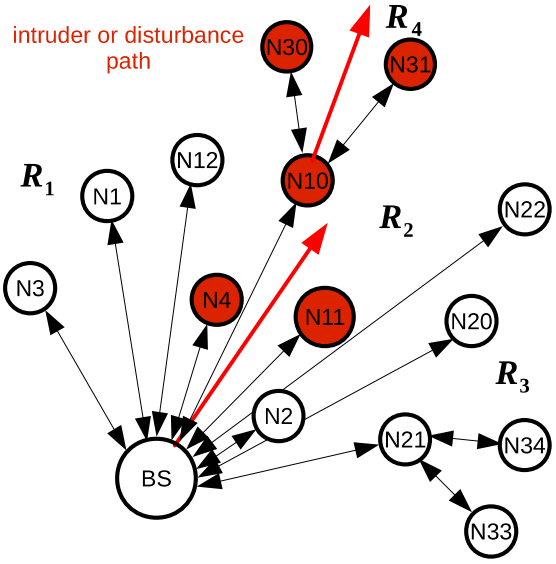

Figure 13 Setup for routing concept and intruder path detection

Due to the EpHESOS protocol the nodes and the base station are pairwise synchronized. Each hop increases the latency by one hop delay and because the nodes are synchronized the delays are known and can be used as a measure against relay attacks. With respect to combating jamming attacks, if we consider Figure 13, it can be clearly seen that, if there is a local network disruption, a path to the malfunctioning nodes can be found. The measures to qualify a disruption are delay variations, RSSI changes, packet loss or similar error-indicating measurements. The routing protocol was designed with communication links to propagate this surveillance information as meta information constantly while the network operates. A fixed latency energy efficient two hop routing network is implemented as proof of concept.

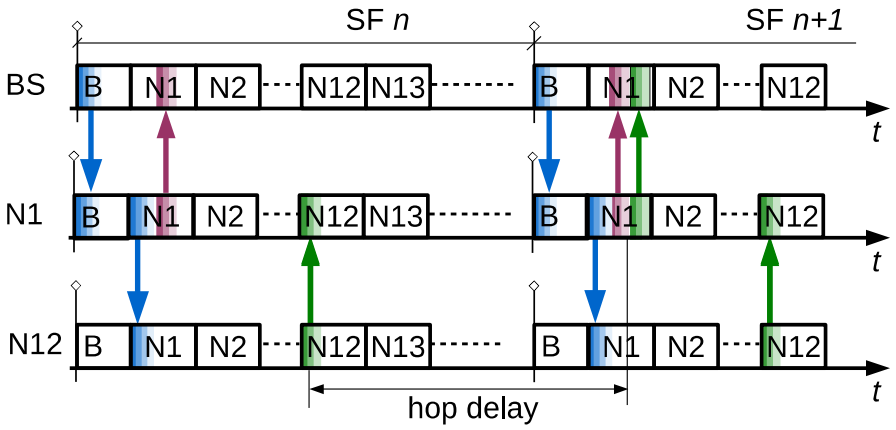

Figure 14 Timing slot organization for routing

The routing concept is developed with a central logic in the base station, controlling, computing, storing and communicating the routing path. All information is collected centrally and distributed as processed information in the form of a trust indicator, the routing path and the trust value of the routing path. In Figure 14 we depict the developed timing structure of the EpHESOS protocol assisting routing. In the continuous mode of EpHESOS, in which each node transmits its data on a regular basis, commands are sent throughout the network via beacons at the start of the superframe or in the time slot of an individual hop node like N1 in Figure 14. This is processed by the BASEBAL algorithm with integrated commands in the EpHESOS framework.

As an add-on to the above described demonstrator “Energy Efficient Secure Communications”, we also developed an **RSSI-based presence detection scheme**. The spatial information of a mobile node is passively collected, supported by nodes only listening to the channel monitored. So-called path nodes are arranged alongside the routes of mobile nodes in a factory or similar. Path nodes have the same architecture as conventional sensor nodes and are participating in the same way in the EPhESOS protocol. As they are pre-installed and static, they do not have the requirement to operate energy autarkic. Thus, they can listen to the network communication throughout all TDMA timeslots and record the RSSI values of each packet. These RSSI values are sent to an edge computing device via the base station.

In order to localize the mobile node without any additional sensor node complexity, the mobile node is not an active part of the localization system. The communication schedule and protocol of the mobile sensor node is performed without any change to the communication peers. Alongside the expected area of mobility, passive listening path nodes are mounted. We used two machine learning algorithms for binary classification if a mobile sensor node is in a predefined cell or not. One algorithm uses SVM and provides a deterministic approach through a convex formulation of the training problem. The second algorithm applies a NN to offer a higher degree of freedom in the solutions. The two classification methods for determining whether a mobile node is inside or outside of a predefined cell, were tested in a garage similar to the soak testing application. A mobile node was mounted at the front of a car while driving with walking speed into a cell, i.e. a parking lot. The mobile node transmited every 0.5 s data to the base station, hence, the sampling time of the RSSI measurements at the guard nodes was the same as the packet transmission time of the node. Figure 15 depicts the measurement setup with the trajectory of the car and the positions of the path nodes.

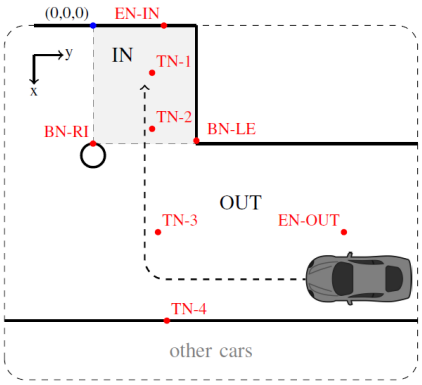

Figure 15 Measurement setup

Figure 16 shows the SVM-estimated position (1 in cell; 0 not in cell) of the node compared to ground truth without postprocessing (a) and with post-processing (b). Post-processing is performed by applying a windowed median filter for binary values, which is based on the assumption of a simple dynamic dependency, i.e., that the mobile sensor node cannot perform abrupt position changes. A more detailed experimental evaluation showed, that using a sample rate of 2 Hz on the

RSSI values, the mean absolute time difference between ground truth cell entering and the estimated cell entering is in the order of 0.58 to 0.74s.

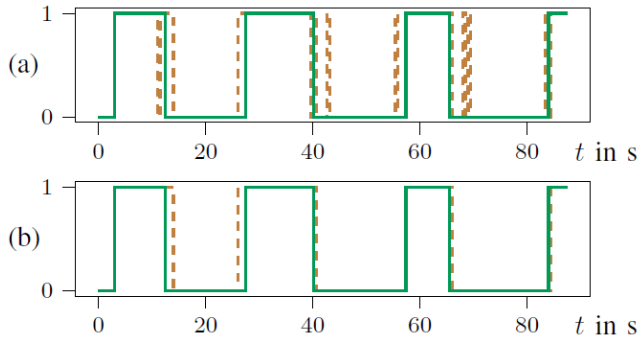

Figure 16 SVM estimated position (1 in cell; 0 not in cell) of the node (dashed line) compared to ground truth (solid line) without postprocessing (a) and with post-processing (b).

3.2.6.1 Link to technology lines

The Energy Efficient Secure Communications demonstrator is based on BB 25.A: Energy efficient security implementation in WSNs and BB23.G PHY Layer Security.

3.2.6.2 Demonstrator public output

It is planned to produce a video demonstrating the security parameter measurement including packet transmission from node to base station and automation system. For the RSSI-based presence detection scheme part of the demonstrator a short video is available demonstrating the proof-of-concept.

3.3 Integration of Demonstrators

This section describes how the six demonstrators are related to each other.

The “core demonstrator” for WP12 is the Vehicle Conditioning (SOAK) demonstrator (section 3.2.1). Except for the Cross-Technology Communication demonstrators (section 3.2.4), all other demonstrators are either fully or partially integrated into it. The Energy Efficient Secure Communications demonstrator (section 3.2.6) realizes the wireless sensor network required for the basic sensing and data transfer functionality. The required secure key exchange for the encryption of the wireless data transfer in the Energy Efficient Secure Communications demonstrator is realized via the OOB Communication demonstrator (section 3.2.5), which is fully integrated. Both, the 3D Sensors positioning demonstrator (section 3.2.2) and the Jamming detection and counteraction demonstrator (section 3.2.3) were planned to be integrated into the Energy Efficient Secure Communications demonstrator during an on-site visit of LCM at GUT premises in March 2020. However, this was not possible due to travel restrictions because of the Corona situation. So currently both demonstrators, the 3D Sensors positioning demonstrator and the Jamming detection and counteraction demonstrator appear as stand-alone demonstrators. However both demonstrators as well as the Energy Efficient Secure Communications demonstrator are fully prepared –with respect to the hardware- and the software interfaces – to be integrated.

The Cross-Technology Communication demonstrator (section 3.2.6) was not planned to be integrated into the other demonstrators. It specifically targets the use case scenario 6 “Configure, check and run a distributed test setup, combining two or more parts of a UUT” in which it is also foreseen that the distributed testing infrastructure is based on different wireless technologies with

no fixed infrastructure for coordination available. The integration of this demonstrator into the Vehicle Conditioning (SOAK) demonstrator would have been too much effort for setting up an appropriate Vehicle Conditioning (SOAK) demonstrator.

4 DISSEMINATION, EXPLOITATION AND STANDARDISATION

Dissemination activities related to the demonstrators from WP 12 can be grouped in two categories:

(i) Publications:

a. Jamming detection and counteraction demonstrator – GUT: Publications [6] and [7]

b. Demonstrators Cross-Technology Communication – TUG: Publications [1], [2], [3]

c. Demonstrator OOB Communication – LCM: Publication: [8]

d. Demonstrator Energy Efficient Secure Communications – JKU: Publication: [5]

(ii) Videos: See the sections 3.3.x.2 Demonstrator public output for descriptions on the existing and planned videos

(iii) Postings on SCOTT's social network channels, e.g. ResearchGate: [9]

Exploitation potential reported by WP12 partners

Exploitable Foreground (description)	Exploitable product(s) or measure(s)	Owner & Other Beneficiary(s) involved	IPR exploitable measures taken or intended
Cross-technology synchronization between off-the-shelf BLE and IEEE 802.15.4 devices		TUG	
Secure dependable energy-efficient WSN for automotive instrumentation	Industrial-grade measurement system for instrumentation in automotive testing,	JKU, LCM (wireless communication) GUT (positioning), AVL	transfer into AVL product development will be planned
Sensor positioning system for ubiquitous testing environments	Embedded cameras with edge computing capabilities together with algorithms for precize 3D sensor positioning	IPR owner - GUT; first business partners AVL (Secure dependable energy-efficient WSN for automotive instrumentation)	transfer into AVL product development is considered (directly by GUT or via a dedicated 3rd party); IPR transfer to a 3rd party set-up to sell the final product
Single-anchor indoor positioning system	Embedded device with reconfigurable antenna and edge computing capabilities together with algorithms for indoor localization	IPR owner - GUT; cooperation with Philips Healthcare, Johnson Controls, Vemco, AVL to make first implementations	IPR transfer to a 3rd party set-up to sell the final product

Exploitable Foreground (description)	Exploitable product(s) or measure(s)	Owner & Other Beneficiary(s) involved	IPR exploitable measures taken or intended
Security Extension for Ultra-Low Latency Wireless Protocol "Ephesos"	Secure and ultra-low latency communication protocol for industrial applicaitons.	LCM, JKU	
Energy efficient real-time routing		JKU	
System Trust Indicator for WSN-based instrumentation system	A set of >10 factors contributing to overall system trust-ability indication	AVL, JKU, LCM	

5 LINK TO TECHNOLOGY LINES

This part of the deliverable describes how the UC work described in this deliverable is linked to the Technology Lines and their Technical Building Blocks (TBB).

TBB \ Demonstrator relation	*SOAK_AVL*	*MPS_GUT*	*SEC JKU*	*CTC_TUG*	*SBA*
BB23.F_LCM	X		X		
BB23.P_GUT	X	X			
BB25.A_JKU	X		X		
BB25.B_NXP-NL					
BB26.A_INDRA					
BB23.G_JKU	X	X	X		
BB24.B_VIF	X				
BB24.F_AVL	X			X	X
BB25.B_NXP-NL	X				
BB25.C_ACCIONA	X				
BB25.E_ACCIONA					
BB26.D_ISEP					
BB23.C_VIF	X				
BB23.K_MGEP					
BB23.L_TECNALIA					
BB23.N_VIF					
BB23.O_NOKIA					
BB23.R_VIF					
BB24.K_VIF					
BB25.F_LCM	X		X		

Table 8 Technology lines link.

6 CONCLUSIONS

This deliverable describes the final status of the six demonstrators in WP12. The implemented technologies are related to different aspects of wireless sensors communication (efficiency, security and interoperability) and localization. The demonstrators have been developed and tested in laboratory conditions and mostly also in the real environment. In addition, component integration (e.g. with AVL PUMA) was achieved in parts.

The results of the demonstrators have been published at scientific venues and videos are and will be available for dissemination to the public.

7 REFERENCES

[1] R. Hofmann, C.A. Boano, and K. Römer. X-Burst: Enabling Multi-Platform Cross-Technology Communication between Constrained IoT Devices. In Proceedings of the 16th IEEE International Conference on Sensing, Communication and Networking (SECON). Boston, MA, USA. June 2019.

[2] H. Brunner, R. Hofmann, M. Schuß, J. Link, M. Hollick, C.A. Boano, and K. Römer. Cross-Technology Broadcast Communication between Off-The-Shelf Wi-Fi, BLE, and IEEE 802.15.4 Devices. In Proceedings of the 17th International Conference on Embedded Wireless Systems and Networks (EWSN), demo session. Lyon, France. February 2020.

[3] D. Grubmair, R. Hofmann, C.A. Boano, and K. Römer. Accurate Cross-Technology Clock Synchronization Among Off-The-Shelf Wireless Devices. In Proceedings of the 17th International Conference on Embedded Wireless Systems and Networks (EWSN), poster session. Lyon, France. February 2020.

[4] Bernhard H., Springer A., Berger A., Priller P.: Life Cycle of Wireless Sensor Nodes in Industrial Environments: 13th IEEE International Workshop on Factory Communication Systems, Trondheim, Norway, Trondheim, Norway, Seite(n) 1-8, 2017

[5] H.-P. Bernhard, A. Springer, “Energy Balanced Routing for Latency Minimized Wireless Sensor Networks“, *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*, Imperia, Italy, June 2018, doi: 10.1109/WFCS.2018.8402350

[6] J. Rewienski, M. Groth, L. Kulas and K. Nyka, "Investigation of continuous wave jamming in an IEEE 802.15.4 network," *2018 22nd International Microwave and Radar Conference (MIKON)*, Poznan, 2018, pp. 242-246, doi: 10.23919/MIKON.2018.8405189

[7] M. Tarkowski et al., "Validation of a virtual test environment for C2X communication under radio jamming conditions," 2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE), Graz, Austria, 2019, pp. 1-5.

[8] Hörmann, L. B.; Kastl, C.; Bernhard, H.-P.; Priller, P. & Springer, A. “Lifetime Security Concept for Industrial Wireless Sensor Networks”, 2020 16th IEEE International Workshop on Factory Communication Systems (WFCS), 2020, to be published.

[9] SCOTT Project https://www.researchgate.net/project/SCOTT-Secure-Connected-Trustable-Things/update/5bbc79eccfe4a76455f94d8d?_iepl%5BviewId%5D=HdeNFQCqsHWUGHCLMqOm2Fll&_iepl%5Bcontexts%5D%5B0%5D=projectUpdatesLog&_iepl%5BinteractionType%5D=projectUpdateDetailClickThrough [last accessed 2020-03-17]

[10] SCOTT Deliverable D12.1 Use Case Specification *"Ubiquitous Testing of Automotive Systems"*, v1.02, 2017-12-18.

A. ABBREVIATIONS AND DEFINITIONS

Term	Definition
BASEBAL	BAckward Structured Energy BAlanced Link
BLE	Bluetooth Low Energy
CCA	Clear Channel Assessment
CTC	Cross-Technology Communication
HLA	Hardware Abstraction Layer
IoT	Internet of Things
MAC	Medium Access Control Layer
NFC	Near-Field-Communication
NN	Neural Network
OOB	Out-of-Band
OS	Operating System
PER	Packet Error Rate
PHY	Physical Layer
PLC	Programmable Logic Controller
RSS	Received Signal Strength
RSSI	Received Signal Strength Indicator
SVM	Support Vector Machine
TDMA	Time Division Multiple Access
UUT	Unit Under Test
WSN	Wireless Sensor Network